UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,441	12/27/2000	Wolfgang Daum	9D-HR-19614-Daum et al	4179

7590 09/21/2006

John S. Beulick
Armstrong Teasdale LLP
ONE METROPOLITAN SQUARE
SUITE 2600
ST. LOUIS, MO 63102

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/748,441	DAUM ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 30 June 2006.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 16-22,24,25 and 27-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 16-20,24,25 and 27-31 is/are rejected.

7)☒ Claim(s) 21,22 and 32 is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 25 July 2002 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 06/30/2006. Claims 16, 25, 28 and 30 have been amended; claim 32 has been added.

Response to Arguments

2. Applicant's arguments filed 06/30/2006 have been fully considered but they are not persuasive.

With respect to the rejection of claims 16-22, 24-25 and 27-31 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement, Applicant states that independent claims 16, 25, 28 and 30 have been amended to address the issue. The amended claims are still not supported by the original disclosure (see figure 7 and corresponding text for discussion of changing the first keying variable which is the shared authentication keying variable).

With respect to the rejection of claims 16, 19-22, 24 and 30 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, Applicant states that independent claims 16 and 30 have been amended to address the issue. The amended claims still do not recite the step(s) for authenticating the appliance message.

With respect to the rejections of claims 16-20, 24-25 and 27-31 under 35 U.S.C. 103(a), Applicant states that Elgamal (5,825,890) describes that the client delivers a master key to the server, and the master key is used by the client and the server to produce session keys. Applicant then argues that (i) Elgamal does not describe or suggest changing a session key by storing a master key at both transmitting and receiving devices; (ii) delivering a master key from a client to a server does not suggest storing a master key at both devices; and (iii) producing a session key does not suggest changing a pre-existing keying variable (page 10, 1st paragraph). First, Elgamal does disclose that the master key is stored by both the client and the server at their respective cache memories (col. 8, lines 34-40). Second, since there is only one valid session key at a time, producing a session key for a new session automatically invalidates the session key that the client and the server have for a previous session.

Applicant argues that there is no motivation to combine the references suggested in the art (page 20, 1st paragraph). Attention is directed to the previous Office Action for suggestion or motivation for combining the references.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (page 20, last paragraph), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 16-22, 24-25 and 27-31 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 16 recites the limitation "changing, within the first appliance, the shared authentication keying variable by installing a master keying variable within the first appliance and the appliance communication center". The limitation is interpreted as either

(a) the master keying variable is the new shared authentication keying variable; or (b) the value of the shared authentication keying variable is automatically changed when a master keying variable is installed. Neither interpretation is supported by the original disclosure (see figure 7 and corresponding text for discussion of changing the shared authentication keying variable). Therefore, the limitation is considered new matter. Claims 25, 28 and 30 are rejected on the same basis as claim 16. Claims that are not specifically addressed are rejected by virtue of their dependency.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 16, 19-22, 24 and 30 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. With respect to claim 16, the omitted step is: authenticating the appliance message as stated in the preamble. Claim 30 is rejected on the same basis as claim 16. Claims that are not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 16-19, 24 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow (6,061,668) in view of Elgamal et al (5,825,890) and Hoffman et al (6,366,682). Sharrow discloses an appliance communication network in which an appliance communication center communicates with different appliances (Abstract; fig. 1, elements 10 and 12-15).

Regarding claims 16-17, 19 and 28, Sharrow discloses a method comprising: applying at an appliance communication center an appliance message to an algorithm to generate a first checksum value, transmitting the appliance message and the first checksum value to an appliance, receiving the appliance message and the first checksum value by the appliance, generating a second checksum value based on the received appliance message, and comparing the first checksum value and the second checksum value to determine the integrity of the appliance message (fig. 2 and corresponding text).

Sharrow does not disclose using a shared message counter shared between the communication center and the appliance, and generating the authentication word using the message, the value of the shared message counter and a shared keying variable shared between the communication center and the appliance. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 26-30), applying a message, the shared message counter, and a shared first keying variable, i.e. a session key, to an authentication algorithm to generate a first authentication word (col. 17, line 56 – col. 18, line 17), and transmitting the first authentication word with the message to a receiver wherein the receiver uses a shared message counter, a shared first authentication keying variable both stored at the receiver and the received message to generate a second authentication word configured to be compared with the first authentication word (col. 18, lines 12-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the method of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance communication center and the appliance, to apply the message, the shared message counter and a shared first keying variable to an authentication algorithm to generate an authentication word, and to transmit the authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Sharrow does not disclose changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center. Elgamal further discloses changing the first shared keying variable by storing a master keying variable at both transmitting and receiving devices and using the master keying variable to generate a new first shared keying variable (col. 7, lines 41-59; col. 8, line 44 – col. 9, line 12; col. 8, lines 57-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to change the Elgamal method further to change the first shared keying variable by storing a master keying variable at both ends of the communication channel and using the master keying variable to generate a new first shared keying variable, as taught by Elgamal, in order to enhance security.

Elgamal discloses maintaining a shared message counter in one-to-one communication. Elgamal does not disclose maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other entities. Hoffman discloses that an entity (i.e., the data processing center) communicates with other entities (BIA devices) and that the entity maintains multiple shared message counters, each of the shared message counter is separately maintained for each of the other entities (fig. 8; col. 29, line 42 - col. 30, line 59). Since the Sharrow appliance communication center communicates with multiple appliances, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow method to maintain, at the appliance communication center, multiple shared message counters, each of the shared message counter is separately maintained for each of the devices, as taught by Hoffman. The motivation for doing so would have been to prevent replay attack when one entity communicates with two or more other entities.

Regarding claims 18 and 29, Elgamal further discloses incrementing the shared message counter, as stored in the receiving side, after receiving a genuine authenticated message at the receiving side (col. 18, lines 24-33).

Regarding claim 24, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

9. Claims 25, 27 and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Elgamal, Hoffman and "Commercial Laundry Services".

Regarding claim 25, Sharrow discloses a system in which an appliance communication center is connected to and communicates with a plurality of appliances via a network wherein data integrity of messages transmitted between the appliance communication center and the appliances are protected using checksums (Abstract; fig. 1, elements 10 and 12-15, figures 2 and 3).

Sharrow does not disclose that the appliance communication center uses and stores a shared message counter shared between the communication center and one of the appliances, generates an authentication word using the message, the value of the shared message counter and a shared keying variable. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 26-30), applying a message, the shared message counter, and a shared first keying variable, i.e. a session key, to an authentication algorithm to generate a first authentication word (col. 17, line 56 – col. 18, line 17), and transmitting the first authentication word with the message to a receiver wherein the receiver uses a shared message counter, a shared first authentication keying variable both stored at the receiver and the received message to generate a second authentication word configured to be compared with the first authentication word (col. 18, lines 12-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the system of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance communication center and the appliance, to apply the message, the shared message counter and a shared first keying variable to an authentication algorithm to generate an authentication word, and to transmit the authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Sharrow does not disclose changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center. Elgamal further discloses changing the first shared keying variable by storing a master keying variable at both transmitting and receiving devices and using the master keying variable to generate a new first shared keying variable (col. 7, lines 41-59;

col. 8, line 44 - col. 9, line 12; col. 8, lines 57-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to change the Elgamal method further to change the first shared keying variable by storing a master keying variable at both ends of the communication channel and using the master keying variable to generate a new first shared keying variable, as taught by Elgamal, in order to enhance security.

Elgamal discloses maintaining a shared message counter in one-to-one communication. Elgamal does not disclose maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other entities. Hoffman discloses that an entity (i.e., the data processing center) communicates with other entities (BIA devices) and that the entity maintains multiple shared message counters, each of the shared message counter is separately maintained for each of the other entities (fig. 8; col. 29, line 42 - col. 30, line 59). Since the Sharrow appliance communication center communicates with multiple appliances, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow method to maintain, at the appliance communication center, multiple shared message counters, each of the shared message counter is separately maintained for each of the devices, as taught by Hoffman. The motivation for doing so would have been to prevent replay attack when one entity communicates with two or more other entities.

Elgamal and Hoffman do not disclose that their counters are non-resettable. The "Commercial Laundry Services" reference discloses using non-resettable counter to insure accountability (see At Jetz, Security is a key). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow system such that the counters are non-resettable, as taught in "Commercial Laundry Services", in order to insure accountability.

Regarding claim 27, Elgamal further discloses incrementing the shared message counter, as stored in the sending side, after transmitting the authenticated message (col. 18, lines 24-30).

Regarding claim 30, Sharrow discloses a method comprising: at an appliance, applying an appliance message to an algorithm to generate a checksum value (fig. 3), and transmitting the appliance message and the checksum by the appliance to an appliance communication center (fig. 3).

Sharrow does not disclose maintaining a shared message counter at the first appliance and the appliance communication center, using the shared message counter and a shared first keying variable to generate the authentication word. Elgamal discloses a method for authenticating a message using a message authentication code (MAC). The Elgamal method includes, among other steps, maintaining a shared sequence number, which meets the limitation of a shared message counter, at both ends of a communication channel (col. 18, lines 26-30), applying a message, the shared message counter, and a shared first keying variable, i.e. a session key, to an authentication algorithm to generate a first authentication word (col. 17, line 56 – col. 18, line 17), and transmitting the first authentication word with the message to a receiver wherein the receiver uses a shared message counter, a shared first authentication keying variable both stored at the receiver and the received message to generate a second authentication word configured to be compared with the first authentication word (col. 18, lines 12-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Elgamal method for authenticating a message using a message authentication code into the system of Sharrow; in particular, it would have been obvious to one of ordinary skill in the art at the time the invention was made to maintain a shared message counter at the appliance communication center and the appliance, to apply the message, the shared message counter and a shared first keying variable to an authentication algorithm to generate an authentication word, and to transmit the authentication word with the message. The motivation for doing so would have been to allow the receiver of a message to authenticate the message.

Sharrow does not disclose changing, within the first appliance, a first keying variable by installing a master keying variable within the first appliance and the appliance communication center. Elgamal further discloses changing the first shared keying variable by storing a master keying variable at both transmitting and receiving devices and using the master keying variable to generate a new first shared keying variable (col. 7, lines 41-59; col. 8, line 44 - col. 9, line 12; col. 8, lines 57-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to change the Elgamal method further to change the first shared keying variable by storing a master keying variable at both ends of the communication channel and using the master keying variable to generate a new first shared keying variable, as taught by Elgamal, in order to enhance security.

Elgamal discloses maintaining a shared message counter in one-to-one communication. Elgamal does not disclose maintaining multiple shared message counters by an entity when the entity communicates with two or more other entities; each of the shared message counters is separately maintained for each of the other entities. Hoffman discloses that an entity (i.e., the data processing center) communicates with other entities (BIA devices) and that the entity maintains multiple shared message counters, each of the shared message counter is separately maintained for each of the other entities (fig. 8; col. 29, line 42 - col. 30, line 59). Since the Sharrow appliance communication center communicates with multiple appliances, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow method to maintain, at the appliance communication center, multiple shared message counters, each of the shared message counter is separately maintained for each of the devices, as taught by Hoffman. The motivation for doing so would have been to prevent replay attack when one entity communicates with two or more other entities.

Elgamal and Hoffman do not disclose that their counters are non-resettable. The "Commercial Laundry Services" reference discloses using non-resettable counter to insure accountability (see At Jetz, Security is a key). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the Sharrow system such that the counters are non-resettable, as taught in "Commercial Laundry Services", in order to insure accountability.

Regarding claim 31, Sharrow further discloses receiving the message at the appliance communication center (fig. 2; col. 3, lines 23-26). Elgamal further discloses applying the shared message counter, as stored in the receiving side, and the received message to an authentication algorithm to generate a second authentication word and comparing the first and second authentication words to determine the authenticity of the message (col. 18, lines 31-38).

10. Claims 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sharrow in view of Elgamal and Hoffman as applied to claim 19 above, and further in view of Kaufman et al ("Network Security Private Communication in a Public World"). Sharrow and Elgamal disclose using a shared message counter to generate the first authentication word in claim 16. Elgamal discloses that the authentication algorithm iteratively performs arithmetic or logical operations (col. 18, lines 4-6). Sharrow and Elgamal do not disclose using a directional code to generate the first authentication word, Kaufman teaches using a directional code for authentication (Section 9.3.5 Privacy and Integrity, p. 242, 3rd par). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the combined method of Sharrow, Elgamal and Hoffman to use a directional code for authentication, as taught by Kaufman. Accordingly, the directional code is used to generate the first authentication word. The motivation for doing so would have been to be able to prevent a reflection attack. Sharrow discloses a working register (col. 5, lines 1-5). Sharrow does not disclose

that the working register comprising at least four bytes, the first three bytes holding the shared message counter the fourth byte holding the directional code. However, the differences between the claimed working register and the working register of Sharrow is a matter of design choice since both store the shared message counter and the directional code.

Allowable Subject Matter

11. Claims 21-22 and 32 would be allowable over the prior art of record if rewritten to overcome the rejections under 35 U.S.C. 112, both first paragraph and second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 7,103,185 to Srivastava et al.

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
9/15/06

Gilbert Z

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100